Director of Central Intelligence
Security Committee
Computer Security Subcommittee

29 October 1979
DCISEC-CSS-M126

1. The one hundred and twenty-sixth meeting of the Computer Security Subcommittee was held at 0930 on 2 October 1979 [redacted] STAT
[redacted] Those attending were: STAT

[redacted] STAT

Mr. James Studer, Army
[redacted] STAT
Mr. Robert Graytock, Department of Justice
Mr. Edward Springer, DoE
Mr. James Schenken, Secret Service

2. The minutes of the 19 July meeting were approved as written.

3. It was reported that the DCI had approved the APEX program. However, this was the only information available, and the scope, details, and impact of what actually has been approved was unknown.

4. The EEI's had not yet been completely coordinated, and it was agreed that the goal is to close this item by the next meeting. It was further agreed that the coordination of the EEI's within the respective agencies need not be extensive, but rather would be selective, at the discretion of the members.

STAT [redacted]

However, DIA has automated files, available on DIAOLS, which will also be used for review against the EEI's. There was some discussion of the particulars of the screening process which will be required.

6. Mr. Studer reported that he had attended a recent meeting of the Data Standards Panel of the Intelligence Information Handling Committee (IIHC). The panel is trying to define, for the purposes of standardization, the security attributes that can be assigned to data files and data elements. He felt that among the most important considerations were:

a. granularity - classification markings down to the field of a record.

b. currency - some indication of the date the information was entered or last updated.

There was some discussion of the potential complexity implied by the granularity and currency requirements. While some agencies currently maintain their files with the desired markings, others leave file management largely to the individual analysts. However, the new regulations will require both currency information and a fine granularity of classification markings, thus implying data base and file managers at the system level.

7. The committee discussed the proposed rewrite of DCID 1/16. It was agreed that although the committee would provide the final determination of policy and technical issues, and could determine the format and outline for the document, there still would need to be a small group who could dedicate the time required to produce a finished product. Thus, CIA, DIA, and NSA will provide nominees for such a group, whose goal will be to dedicate approximately two days per week toward executing the rewrite, as directed by the committee. Both NSA and CIA provided nominees for the working group, DIA indicating that they would provide a specific name at a later date. The discussions highlighted the need for a mechanism (e.g., a questionnaire) for documenting problems that exist with the present document, desired improvements, additions, etc. The agreement reached was that the three-member working group would be responsible for drafting a letter, for the committee's review, explaining the committee's intent and soliciting comments/ideas for the rewrite. Some cautionary comments were provided by the NSA member, primarily:

a. The rewrite should be a revision of the existing DCID, not a completely new document.

b. Although the final document may include specific technical guidelines as appendices, the basic policy statements should be reasonably brief.

8. In accordance with discussions at the previous meeting concerning contractor access to sensitive information, CIA distributed copies of their contractor security manual. DIA's version of such a manual, DIAM 50-5, is presently being printed. Further discussion followed concerning the problem of contractors who handle or process SCI, especially those who have concurrent contracts with several Intelligence Community agencies. The obvious need is for a wide range of standardized procedures, physical and personnel security requirements, computer security requirements, etc. Additionally, the advantage of a cognizant agency for each such contractor was recognized. (The CIA member stated that they had drafted an issue paper in this area to Mr. Gambino, CIA.) It was suggested that DCID 1/16 provides the basic policy to cover these situations, and that an appropriate annex to the Industrial Security Manual could be written. The pros and cons of this approach were argued, the biggest problem being the aspect of having DLA perform the inspection of SCI facilities. It was finally agreed that the CSS will draft the policy, guidelines, and proposed procedures for contractors who process SCI belonging to two or more Intelligence Agencies. Several potential procedures were discussed, but it was resolved that the CSS would provide the basic policy and procedures in the revised DCID 1/16.

9. There was considerable discussion concerning the scope of the computer security concerns, and how the implementation of ADP technology into applications such as facsimile devices and word processors, affects the role of the CSS. Since these devices and their internal memories are often overlooked, Mr. Studer (Army) and [redacted] (CIA) volunteered to draft a news note to the community discussing the security concerns of such devices. STAT

10. The next meeting was set for 1 November 1979 [redacted] STAT

[redacted] STAT

Executive Secretary
Computer Security Subcommittee